

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-210025

(43) 公開日 平成10年(1998) 8月7日

(51) Int.Cl.⁶ 識別記号
 H 0 4 L 9/08
 G 0 9 C 1/00 6 6 0
 H 0 4 L 9/14

F I
 H 0 4 L 9/00 6 0 1 Z
 G 0 9 C 1/00 6 6 0 F
 H 0 4 L 9/00 6 0 1 E
 6 4 1

審査請求 未請求 請求項の数 6 O L (全 13 頁)

(21) 出願番号 特願平9-296513

(22) 出願日 平成9年(1997)10月29日

(31) 優先権主張番号 特願平8-290373

(32) 優先日 平8(1996)10月31日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 福島 能久

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 弁理士 中島 司朗

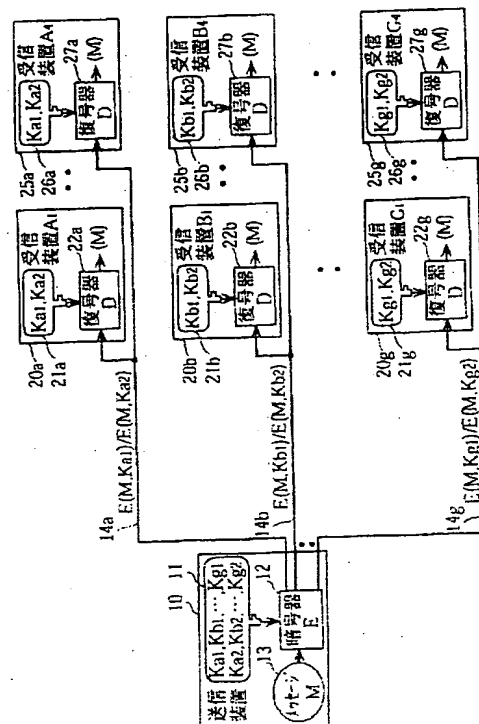
最終頁に続く

(54) 【発明の名称】 暗号通信システム

(57) 【要約】

【課題】 第三者の攻撃による秘密鍵の推定を困難にすると共に、秘密鍵が解読された場合のシステムへの影響を小さく抑えることが可能な暗号通信システムを提供する。

【解決手段】 1台の送信装置10と7つのグループA～Gに分類される合計28台の受信装置A1～G4からなる暗号通信システムにおいて、各グループには14種類の相異なる秘密鍵から重複しないで選択した2個の秘密鍵を予め配布しておく。送信装置10は、各グループについて配布された2個の秘密鍵のいずれかを用いて同一のメッセージMを暗号化し、対応するグループの受信装置に送信する。受信装置それぞれは、受信した暗号文に対して自己が属するグループに配布された2個の秘密鍵それぞれを用いて復号化し、得られた2個の復号文それぞれについて一定の規則性が存在するか否かを判断することで、正しい復号文を特定する。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 n 台の受信装置と、それら n 台の受信装置に対してデジタル情報を伝送する1台の送信装置とからなる暗号通信システムであって、
 前記 n 台の受信装置は m 個のグループに分類され、各グループには $m \times k$ 個の異なる秘密鍵から重複しないで選択された k 個の秘密鍵が配布されており、
 前記送信装置は、
 前記 $m \times k$ 個の秘密鍵と同一の秘密鍵を、配布されたグループに対応づけて予め記憶する秘密鍵記憶手段と、
 前記 m 個のグループそれぞれについて、前記秘密鍵記憶手段に記憶された各グループに対応する k 個の秘密鍵から1個を選択して読み出す秘密鍵選択手段と、
 読み出された m 個の秘密鍵それぞれを用いて1つの平文を暗号化する暗号化手段と、
 前記暗号化手段によって得られた m 個の暗号文を各暗号文が生成される際に用いられた秘密鍵と同一の秘密鍵を有する受信装置それぞれに伝送する伝送手段とを備え、
 前記 n 台の受信装置それぞれは、
 この受信装置が属するグループに配布された前記 k 個の秘密鍵を予め記憶する秘密鍵記憶手段と、
 前記送信装置から伝送されてきた暗号文を受信する受信手段と、
 受信した前記暗号文に対して前記 k 個の秘密鍵それぞれを用いて復号化する復号手段と、
 前記復号手段によって得られた復号文それぞれについて予め決められた規則性が存在するか否かを判断し、少なくとも一つの復号文に規則性が存在する場合には、それら規則性が存在する復号文のひとつを前記平文と同一と認定する判断手段とを備えることを特徴とする暗号通信システム。

【請求項2】 前記送信装置の伝送手段は、前記暗号文に前記規則性を示す暗号文を添付して前記伝送を行ない、
 前記受信装置の判断手段は、前記送信装置から伝送されてきた前記規則性を示す暗号文に基づいて前記判断をすることを特徴とする請求項1記載の暗号通信システム。

【請求項3】 デジタル情報を n 台の受信装置に伝送する送信装置であって、
 前記 n 台の受信装置は m 個のグループに分類され、各グループには $m \times k$ 個の異なる秘密鍵から重複しないで選択された k 個の秘密鍵が配布され、各受信装置は自己が属するグループに配布された k 個の秘密鍵を有し、
 前記送信装置は、
 前記 $m \times k$ 個の秘密鍵と同一の秘密鍵を、配布されたグループに対応づけて予め記憶する秘密鍵記憶手段と、
 前記 m 個のグループそれぞれについて、前記秘密鍵記憶手段に記憶された各グループに対応する k 個の秘密鍵から1個を選択して読み出す秘密鍵選択手段と、
 読み出された m 個の秘密鍵それぞれを用いて1つの平文

を暗号化する暗号化手段と、

前記暗号化手段によって得られた m 個の暗号文を各暗号文が生成される際に用いられた秘密鍵と同一の秘密鍵を有する受信装置それぞれに伝送する伝送手段とを備えることを特徴とする送信装置。

【請求項4】 前記伝送手段は、前記暗号文に元の平文についての規則性を示す暗号文を添付して前記伝送を行なうことを特徴とする請求項3記載の送信装置。

【請求項5】 1台の送信装置から伝送されてくるデジタル情報を受信する受信装置であって、
 予め配布された k 個の秘密鍵を記憶する秘密鍵記憶手段と、

前記 k 個の秘密鍵のいずれかを用いて暗号化された暗号文を前記送信装置から受信する受信手段と、
 受信した前記暗号文に対して前記 k 個の秘密鍵それぞれを用いて復号化する復号手段と、

前記復号手段によって得られた復号文それぞれについて予め決められた規則性が存在するか否かを判断し、少なくとも一つの復号文に規則性が存在する場合には、それら規則性が存在する復号文のひとつを正しい復号文と認定する判断手段とを備えることを特徴とする受信装置。

【請求項6】 前記受信手段は、前記暗号文と共に前記規則性を示す暗号文をも受信し、

前記判断手段は、前記規則性を示す暗号文に基づいて前記判断をすることを特徴とする請求項5記載の受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル化された文書、音声、画像、プログラムなどのデータを伝送媒体や記録媒体を介して暗号伝送するシステムに関し、特に、1台の送信装置が秘密鍵を用いて複数の受信装置に暗号伝送する技術に関する。

【0002】

【従来の技術】従来、デジタル化された文書、音声、画像、プログラムなどのデータを秘密鍵で暗号化し伝送媒体を介して通信したり、記録媒体を介して記録・再生したりする秘密鍵暗号通信システムにおいては、送信装置及び受信装置それぞれは、予め装置間で定めた1個の共通の秘密鍵を用いて暗号化及び復号化を行なっている。

【0003】つまり、送信装置及び受信装置それぞれは、複数の秘密鍵を有している場合であっても、通信を行なう直前においては、1個の秘密鍵を特定し、それを用いることとしている。これは、送信装置から送られた暗号文が受信装置において確実に復号されることを保証するためである。

【0004】

【発明が解決しようとする課題】しかしながら、このような従来の暗号通信システムでは、通信システムの形態

が1対多、即ち、1台の送信装置が多数の受信装置に情報を提供するような形態の場合には、もし秘密鍵が解読されたときには全ての受信装置について新たな秘密鍵を設定し直さなければならず、システム構築の変更という多大な作業が強いられる。

【0005】例えば、もし、1台の放送局と、その放送局から提供される番組を受信する100台の受信機とが有していた秘密鍵が解読された場合には、その放送局及び100台の受信機に記憶されている全ての秘密鍵を変更しなければならない。つまり、1台の送信装置と1台の受信装置間での通信の盗聴によって秘密鍵が解読された場合であっても、それら2台の装置だけでなく、同じ秘密鍵を共有し合う全ての受信装置に影響が及んでしまう。

【0006】そこで、本発明は上記問題点を鑑みてなされたものであり、第三者の攻撃による秘密鍵の推定を困難にすると共に、秘密鍵が解読された場合のシステムへの影響を小さく抑えることが可能な暗号通信システムを提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するために、本発明に係る暗号通信システムは、1台の送信装置と複数のグループ化された受信装置からなる暗号通信システムであって、各グループには相異なる複数の秘密鍵から重複しないで選択した2個以上の秘密鍵を予め配布しておき、その送信装置は、各グループについて1個ずつ選択した秘密鍵それぞれを用いて1つの平文を暗号化し、得られた暗号文を対応するグループに属する受信装置に送信する。受信装置それぞれは、受信した暗号文に対して自己が属するグループに配布された複数の秘密鍵それぞれを用いて復号化し、得られた復号文それぞれについて一定の規則性が存在するか否かを判断することで、正しい復号文を特定する。

【0008】ここで、送信装置は、前記規則性を示す暗号文を前記暗号文に添付して各受信装置に送信することもできる。

【0009】

【発明の実施の形態】

（実施の形態1）以下、本発明に係る暗号通信システムの実施の形態1について図面を用いて詳細に説明する。本暗号通信システムは、秘密鍵が解読された場合であっても、それによる被害規模を抑えることができることを特徴とする。

【暗号通信システムの概要】図1は、実施形態1に係る暗号通信システム全体のシステム構成と暗号通信の原理を説明するための図である。

【0010】本システムは、1台の送信装置10と、その送信装置10から一方向で伝送される伝送情報を受信する28台の受信装置A1～G4から構成される。28台の受信装置A1～G4は、4台で1つのグループを形成す

る合計7つのグループA～Gのいずれかに属する。具体的には、28台の受信装置A1～G4は、バスライン14aに接続されたグループAに属する4台の受信装置A1～A4（うち2台のみが図示されている。）、バスライン14bに接続されたグループBに属する4台の受信装置B1～B4（うち2台のみが図示されている。）、バスライン14gに接続されたグループGに属する4台の受信装置G1～G4（うち2台のみが図示されている。）からなる。

【0011】送信装置10は、全ての受信装置A1～G4に伝えるべきメッセージ13と、14個の相異なる秘密鍵11と、1個の暗号器12とを備え、独立して接続された7本のバスライン14a～14gを用いることで、グループ単位、即ち、4台の受信装置ごとに、一斉同報することができる。受信装置A1～G4それぞれは、2個の秘密鍵21a～21g、26a～26gと、上記暗号器12に対応する（逆変換をする）1個の復号器22a～22g、27a～27gとを備える。

【0012】本システムの目的は、秘密鍵を用いた暗号通信により、1台の送信装置10が28台の受信装置A1～G4に対して1つの（同一の）メッセージMを伝えることである。まず、送信装置10が備える14個の秘密鍵11と各受信装置が備える2個の秘密鍵との関係（秘密鍵の配布形態）を説明する。

【0013】7つのグループA～Gそれぞれには、相異なる14種類の秘密鍵の中から重複しないで選択した2個の秘密鍵を予め配布しておく。つまり、グループAには秘密鍵Ka1及びKa2を配布し、グループBには秘密鍵Kb1及びKb2を配布し、...、グループGには秘密鍵Kg1及びKg2を配布しておく。そして、各受信装置A1～G4それぞれは、自己が属するグループに配布された2個の秘密鍵を記憶しておく。

【0014】一方、送信装置10は、7つのグループA～Gに配布されたものと同一の14個の秘密鍵を各グループに対応づけて記憶しておく。このようにして、14個の秘密鍵は、同一のグループに属する受信装置間では共通化され、異なるグループに属する受信装置間では、共通化されないようにしている。

【0015】次に、送信装置10が28台の受信装置A1～G4に伝送する具体的な暗号文の内容を説明する。送信装置10が28台の受信装置A1～G4に伝送する暗号文は、本図のバスライン14a～14gに示されている通りである。ここで、記号E（M，K）は、平文Mに対して暗号鍵Kを用いて暗号アルゴリズムEに基づいて暗号化して得られた暗号文を意味する。同様に、記号D（C，K）は、暗号文Cに対して復号鍵Kを用いて復号アルゴリズムDに基づいて復号化して得られた復号文を意味する。

【0016】すなわち、送信装置10は、バスライン14aを介してグループAに属する4台の受信装置A1～

A4に対しては暗号文E (M, Ka1) 又はE (M, Ka2) (本図では、E (M, Ka1) / E (M, Ka2) と記されている) を伝送し、バスライン14bを介してグループBに属する4台の受信装置B1~B4に対しては暗号文E (M, Kb1) 又はE (M, Kb2) を伝送し、バスライン14gを介してグループGに属する4台の受信装置G1~G4に対しては暗号文E (M, Kg1) 又はE (M, Kg2) を伝送する。

【0017】具体的には、送信装置10は、グループAに対しては、グループAに配布された2個の秘密鍵(Ka1及びKa2)のいずれかをランダムに選択し、それを用いてメッセージMを暗号器12で暗号化し、得られた暗号文E (M, Ka1) 又はE (M, Ka2) をグループAに属する4台の受信装置A1~A4に一斉同報する。同様に、グループBに対しては、グループBに配布された2個の秘密鍵(Kb1及びKb2)のいずれかを選択し、それを用いてメッセージMを暗号器12で暗号化し、得られた暗号文E (M, Kb1) 又はE (M, Kb2) をグループBに属する4台の受信装置B1~B4に一斉同報する。このようにして、グループごとに異なる暗号文を順次、一斉同報していく。

【0018】一方、受信装置A1~G4それぞれは、受信した暗号文に対して自己が保有する2個の秘密鍵それぞれを用いて復号化し、得られた2種類の復号文の少なくとも1つが信頼できる内容であるならば、その復号文は送信装置10が伝えてきたメッセージMであり、かつ、その復号文を得るために用いた秘密鍵は送信装置10が用いたものと同一と認定する。

【0019】具体的には、受信装置20aであれば、受信した暗号文(E (M, Ka1) 又はE (M, Ka2))に対して、秘密鍵Ka1及びKa2それぞれを用いて復号化し、得られた2個の復号文について、少なくとも1つが信頼できるか否かを、その内容に一定の規則性が存在するか否かで判断する。なお、「一定の規則性」の具体的な基準は後述する。

【0020】以上のように、本暗号通信システムによって、1つのメッセージMが1台の送信装置10から28台の受信装置20aに秘密伝送されたが、このシステムには大きく2つの特徴がある。第1に、異なるグループに属する受信装置間では、秘密鍵が共通化されていないことである。

【0021】従って、もし、1つのグループに配布された秘密鍵が不正者によって解読された場合であっても、他のグループに属する受信装置は影響を受けない、即ち、秘密鍵の変更を強いられないという利点がある。第2に、1つのグループには2個の秘密鍵が配布されているが、実際に用いられる秘密鍵は、それらから選択された1個のみである。

【0022】従って、もし、その1個の秘密鍵が不正者によって解読された場合であっても、以降の伝送におい

ては残る1個の秘密鍵を採用することにより、たとえ同一グループに属する受信装置であっても、秘密鍵を入れ替えることなく秘密通信を継続していくことができる。

【具体的な構成】図2は、図1に示された暗号通信システムにおける送信装置10と1台の受信装置20aのみに着目し、それらの詳細な構成を示すブロック図である。

【0023】送信装置100は、図1における送信装置10に相当し、デジタル著作物101、秘密鍵記憶部103、秘密鍵選択部104、3個の暗号器102、105、107、メッセージ生成部106及び3個の送信部110~112から構成される。この送信装置100は、自己が保有するデジタル著作物を暗号化して受信装置A1に転送することを最終的な目的とし、そのために、暗号化されたデジタル著作物Cdの他に、2種類の暗号文、即ち、そのデジタル著作物の暗号化に用いた1個の秘密鍵を暗に伝えるための暗号文Caと、その秘密鍵を特定するための判断基準となる一定の規則性を伝えるための暗号文Cmとを併せて受信装置A1に送信する。

【0024】デジタル著作物101は、デジタル化された文書、音声、画像、プログラムなどのデータを予め保持しているハードディスク等である。秘密鍵記憶部103は、図1における秘密鍵11に相当し、全てのグループA~Gに配布されたものと同一の14個の秘密鍵を、配布されたグループに対応づけて予め記憶する半導体メモリ等である。

【0025】秘密鍵選択部104は、上記3つの暗号文の生成・送信に先立ち、送信先となる受信装置が属するグループに対応する2個の秘密鍵のいずれかをランダムに選択して秘密鍵記憶部103から読み出し、それを2個の暗号器102及び105それぞれに伝える。具体的には、送信先が受信装置A1の場合には、秘密鍵Ka1又はKa2を選択して秘密鍵記憶部103から読み出し、暗号器102及び105に送る。

【0026】暗号器102は、秘密の暗号アルゴリズムE1に基づく暗号化をするIC等であり、デジタル著作物101からブロック単位でデジタルデータDataを読み出し、それに対して秘密鍵選択部104から送られてきた秘密鍵Ka1又はKa2で暗号化し、得られた暗号文Cd (=E1(Data, Ka1) / E1(Data, Ka2)) を送信部110に送るという処理をデジタル著作物101全てについて繰り返す。

【0027】メッセージ生成部106は、図1におけるメッセージ13に相当し、送信先のグループが異なるごとに新たな1個の乱数を発生し、メッセージMとして保持する乱数発生器等である。なお、本実施形態においては、メッセージMは、上記デジタル著作物101の暗号化に用いた秘密鍵を受信装置A1に伝達するためのキャリアとして用いられるダミーデータであり、その内容は重要でない。

【0028】暗号器105は、秘密の暗号アルゴリズムE2に基づく暗号化をするIC等であり、メッセージ生成部106に保持されたメッセージMを読み出し、それに対して秘密鍵選択部104から送られてきた秘密鍵Ka1又はKa2で暗号化し、得られた暗号文Ca(=E2(M, Ka1)/E2(M, Ka2))を送信部111に送る。

【0029】暗号器107は、秘密の暗号アルゴリズムE3に基づく暗号化をするIC等であり、メッセージ生成部106に保持されたメッセージMを読み出し、そのメッセージMに対してそのメッセージMを暗号鍵として暗号化し、得られた暗号文Cm(=E3(M, M))を送信部112に送る。送信部110、111、112は、並列to直列変換器や増幅器等からなり、それぞれ、バスライン120、121、122を介して上記3種類の暗号文Cd、Ca、Cmを受信装置A1に送信する。なお、3本のバスライン120~122をまとめたものが図1における1本のバスライン14aに相当する。

【0030】一方、受信装置A1は、図1における受信装置20aに相当し、5個の復号器201、221、222、231、232、2個の秘密鍵記憶部220、230、2個の判定部223、233、総合判定部203、秘密鍵選択部202、3個の受信部210~212から構成される。この受信装置A1は、送信装置100から送られてきた暗号化デジタル著作物Cdを復号化して利用することを最終的な目的とし、その復号のために用いるべき秘密鍵、即ち、送信装置100が用いた秘密鍵は、暗号化デジタル著作物Cdと共に受信した2種類の暗号文Ca及びCmから特定する。

【0031】受信部210、211、212は、直列to並列変換器等からなり、それぞれ、バスライン120、121、122を介して上記3種類の暗号文Cd、Ca、Cmを受信する。復号器201は、送信装置100が備える暗号器102の暗号アルゴリズムE1の逆変換である秘密の復号アルゴリズムD1に基づく復号化をするIC等であり、秘密鍵選択部202から秘密鍵Ka1又はKa2が与えられた場合には、受信部210から送られてきた暗号文Cdに対して、その秘密鍵を用いて復号化することにより、元のデジタル著作物のブロックデータDataに復元する。

【0032】なお、この復号器201は、送信装置100から繰り返し暗号化デジタル著作物Cdが送られてくる限り、その復号化を繰り返す。また、秘密鍵選択部202から秘密鍵が与えられない場合には、秘密鍵の特定に失敗したものと認識し、暗号化デジタル著作物Cdの復号化は行なわない。秘密鍵記憶部220、復号器221、復号器222及び判定部223からなる1組の回路群は、送信装置100で用いられた秘密鍵がKa1であるか否かを判定することを目的とし、一方、秘密鍵記憶部230、復号器231、復号器232及び判定部233

からなる他の1組の回路群は、送信装置100で用いられた秘密鍵がKa2であるか否かを判定することを目的とする。これら2組の回路群は、秘密鍵記憶部220及び230に記憶された1個の秘密鍵が異なる点を除いて基本的な構成及び機能は同一である。従って、一方の組のみ詳述する。

【0033】秘密鍵記憶部220は、図1における秘密鍵21aに相当し、秘密鍵Ka1を予め記憶する半導体メモリ等である。復号器221は、送信装置100が備える暗号器105の暗号アルゴリズムE2の逆変換である秘密の復号アルゴリズムD2に基づく復号化をするIC等であり、図1における復号器22aに相当し、受信部211から送られてきた暗号文Caに対して秘密鍵記憶部220から読み出した秘密鍵Ka1を用いて復号化し、得られた復号文M1(=D2(Ca, Ka1))を判定部223及び復号器222に送る。

【0034】復号器222は、送信装置100が備える暗号器107の暗号アルゴリズムE3の逆変換である秘密の復号アルゴリズムD3に基づく復号化をするIC等であり、受信部212から送られてきた暗号文Cmに対して復号器221から送られてきた復号文M1を復号鍵として復号化し、得られた復号文M11(=D3(Cm, M1))を判定部223に送る。

【0035】判定部223は、比較器及びセクタ等からなり、復号器221から送られてきた復号文M1と復号器222から送られてきた復号文M11とが一致するか否かを判定し、一致する場合にはその復号文M1を、一致しない場合には「0」を、総合判定部203に出力する。ここで、一致する場合(M1=M11)とは、送信装置100において選択され用いられた秘密鍵がKa1である場合に相当する。その理由は、以下の通りである。

【0036】いま、送信装置100において、秘密鍵選択部104は秘密鍵Ka1を選択したとする。すると、以下が成立する。

$$Ca = E2(M, Ka1) \quad \text{—式1}$$

$$Cm = E3(M, M) \quad \text{—式2}$$

よって、受信装置A1の復号器221が出力する復号文M1は、式1を用いることにより、以下の通りとなる。

【0037】

$$\begin{aligned} M1 &= D2(Ca, Ka1) \\ &= D2(E2(M, Ka1), Ka1) \\ &= M \quad \text{—式3} \end{aligned}$$

一方、受信装置A1の復号器222が出力する復号文M11は、式2と式3を用いることにより、以下の通りとなる。

【0038】

$$\begin{aligned} M11 &= D3(Cm, M1) \\ &= D3(E3(M, M), M) \\ &= M \quad \text{—式4} \end{aligned}$$

よって、式3と式4とから、以下が成立する。

M1=M11. 一式5

なお、同様にして、もう1組の回路群の判定部233は、復号器231から送られてきた復号文M2と復号器232から送られてきた復号文M22とが一致するか否かを判定し、一致する場合にはその復号文M2を、一致しない場合には「0」を、総合判定部203に出力する。

【0039】総合判定部203は、論理和回路及びセレクタ等からなり、判定部223及び判定部233から出力された復号文に基づいて、受信した暗号化デジタル著作物Cdの復号化に用いるべき復号鍵(Ka1及びKa2のいずれか)を特定する指示を、又は、復号鍵が見当たらない旨の指示を秘密鍵選択部202に送る。具体的には、判定部223が「0」でない復号文M2を出力した場合には判定部233の出力いかに拘わらず秘密鍵Ka1を選択する指示「1」を、判定部223が「0」を出力し、かつ、判定部233が「0」でない復号文M2を出力した場合には秘密鍵Ka2を選択する指示「2」を、その他の場合には復号鍵が見当たらない旨の指示「0」を、それぞれ秘密鍵選択部202に送る。

【0040】秘密鍵選択部202は、セレクタ等からなり、総合判定部203からの3種類の指示「0/1/2」に基づいて、それぞれ、復号器201に秘密鍵を出力しない/秘密鍵Ka1を出力する/秘密鍵Ka2を出力する。秘密鍵選択部202は、送信装置100から暗号化デジタル著作物Cdが繰り返し送信されてくる間、その出力を継続する。

【0041】なお、判定部223(233)は復号文M1(M2)と復号文M11(M22)とが一致しない場合に「0」を出力し、その結果、総合判定部203は、その不一致に係る秘密鍵Ka1(Ka2)は送信装置100において選択された秘密鍵ではないとして上記処理をしているが、これは、本システムに採用されているような暗号(復号)アルゴリズムが通常持つ以下の性質を利用している。

【0042】つまり、「暗号文に対して本来用いるべき秘密鍵とは異なる秘密鍵を復号鍵として復号化した場合に得られる復号文は、元の平文とは異なる。」という性質である。

【暗号通信システムの動作】次に、以上のように構成された本暗号通信システムの動作を説明する。

【0043】図3は、送信装置100の動作手順を示すフローチャートである。送信装置100は、7つのグループA～Gそれぞれについて以下の処理(ステップS51～S53)を繰り返す(ステップS50～S54)。なお、ステップS51～S53に記入されている記号・式は、グループAに対する処理の場合におけるものであり、以下、その場合のみについて説明する。

【0044】まず、秘密鍵選択部104は、グループAに対応する2個の秘密鍵Ka1及びKa2からランダムに1個を選択し、暗号器102及び暗号器105に送る(ス

テップS51)。次に、暗号器102は上記ステップS51で選択された1個の秘密鍵Ka1/Ka2を用いてデジタル著作物101のブロックデータDataを暗号化することにより暗号文Cdを生成し、暗号器105は同じ1個の秘密鍵Ka1/Ka2を用いてメッセージ生成部106で生成されたメッセージMを暗号化することにより暗号文Caを生成し、暗号器107は同じメッセージMを暗号鍵としてそのメッセージMを暗号化することにより暗号文Cmを生成する(ステップS52)。これら3つの暗号化は同時並列に行われる。

【0045】最後に、3つの送信部110、111、112それぞれは、上記ステップS52で得られた3つの暗号文Cd、Ca、Cmそれぞれをバスライン120、121、122それぞれを介してグループAに属する4台の受信装置A1～A4に一斉同報する(ステップS54)。このようにしてグループAに対する送信が終了すると、送信装置100は、次にグループBに対しても同様の送信処理を行うというように、順次7つのグループA～G全てに対して同様の処理を繰り返していく(ステップS50～S54)。

【0046】図4は、受信装置A1の動作手順を示すフローチャートである。なお、他の受信装置A2～A4の動作手順も基本的には本図と同じである。まず、受信部210、211、212は、それぞれ、送信装置100からバスライン120、121、122を介して送られてきた3つの暗号文Cd、Ca、Cmを受信し、復号器201、復号器221及び復号器231、復号器222及び復号器232に送る(ステップS60)。

【0047】次に、第1段階の復号化として、受信部211から送られてきた暗号文Caに対して、復号器221は秘密鍵記憶部220から読み出した秘密鍵Ka1を用いて復号化することにより復号文M1を生成すると同時に、復号器231は秘密鍵記憶部230から読み出した秘密鍵Ka2を用いて復号化することにより復号文M2を生成する(ステップS61)。

【0048】続いて、第2段階の復号化として、受信部212から送られてきた暗号文Cmに対して、復号器222は復号器221が生成した復号文M1を復号鍵として用いて復号化することにより復号文M11を生成し、これと同時並列に、復号器232は復号器231が生成した復号文M2を復号鍵として用いて復号化することにより復号文M22を生成する(ステップS62)。

【0049】そして、判定部223は復号器221が生成した復号文M1と復号器222が生成した復号文M11とが一致するか否かを判定し、一致する場合には復号文M1を、一致しない場合には「0」を総合判定部203に出力し、これと同時並列に、判定部233は復号器231が生成した復号文M2と復号器232が生成した復号文M22とが一致するか否かを判定し、一致する場合には復号文M2を、一致しない場合には「0」を総合判定

部203に出力する(ステップS63、S64)。

【0050】その結果、判定部223から一致した旨の通知(復号文M1)を受けた場合には、総合判定部203は、その通知を判定部233からの通知に優先させ、秘密鍵選択部202に対して秘密鍵Ka1を選択する旨の指示「1」を送る。従って、復号器201は、受信部210から送られてきた暗号文Cdに対して秘密鍵選択部202から送られてきた秘密鍵Ka1を用いて元のデジタル著作物Dataに復号化する(ステップS65)。

【0051】一方、判定部223から一致しない旨の通知(「0」)を受けた場合には、総合判定部203は、さらに判定部233から受けた通知内容を判断し、その結果、一致した旨の通知(復号文M2)であるときには、秘密鍵選択部202に対して秘密鍵Ka2を選択する旨の指示「2」を送る。従って、復号器201は、受信部210から送られてきた暗号文Cdに対して秘密鍵選択部202から送られてきた秘密鍵Ka2を用いて元のデジタル著作物Dataに復号化する(ステップS66)。

【0052】判定部223及び判定部233のいずれからも一致しない旨の通知(「0」)を受けた場合には、総合判定部203は、秘密鍵選択部202に対してその旨の通知「0」を送る。従って、復号器201は、受信部210から送られてきた暗号文Cdに対して復号化を行なわない(ステップS66)。以上のように、本実施形態によれば、7つのグループそれぞれに14種類の相異なる秘密鍵から重複しないで選択した2個の秘密鍵を予め配布しておき、送信装置100は、各グループにつき任意に選択した1個の秘密鍵を用いて暗号化することで、デジタル著作物101及びメッセージMを秘密にして28台の受信装置A1～E4に伝達することができる。

【0053】この方式によれば、例えば、バスライン14aを繰り返し盗聴することで1個の秘密鍵Ka1が不正者に解読された場合であっても、他のグループB～Gに属する受信装置は、その秘密鍵Ka1と異なる秘密鍵を用いているので、それによる影響を受けることなく通信を継続することができる。さらに、送信装置100は、解読された秘密鍵Ka1を用いることなく、残る秘密鍵Ka2を用いることで、グループAに属する受信装置との通信を継続することができる。

【0054】つまり、1個の秘密鍵が漏洩したり解読された場合であっても、送信装置及び全ての受信装置は、新たな秘密鍵の配布を受けて記憶したり、記憶すべき秘密鍵を更新したりすることなく、秘密通信を継続することができる。以上、本発明に係る暗号通信システムについて、実施形態に基づいて説明したが、本発明はこれら実施形態に限られないことは勿論である。即ち、

(1) 本実施形態では、暗号通信システムのネットワーク形態はスター型であり、1台の送信装置が各受信装置ごとに異なる暗号文を送信したが、本発明は、このようなネットワーク形態に限らない。1本の同軸ケーブルに

送信装置及び全ての受信装置が接続されたバス型のネットワークであって、1台の送信装置が複数の受信装置に対して全ての受信装置向けの暗号文をまとめて一斉同報してもよい。

(2) また、本暗号通信システムにおける通信媒体は有線のバスライン14a～14gであったが、CD-ROM等の記録媒体であってもよい。

【0055】図5は、本発明に係る暗号通信システムの通信媒体がCD-ROM250である場合における、送信装置によって書き込まれたCD-ROM250の内容を示す図である。送信装置(CD-ROMライター)は、各グループに対応して予め定められた7つの記録位置251～257それぞれに、各グループ充てに送信する3つの暗号文Cd258、Ca259、Cm260を記録しておき、一方、受信装置(CD-ROMドライブ)は、自己が属するグループに対応する記録位置に記録された3つの暗号文Cd258、Ca259、Cm260を読み出し、デジタル著作物Dataに復号化する、という暗号通信システムであってもよい。

(3) また、本実施形態では、3種類の異なる暗号アルゴリズムが用いられたが、これらは同一であってもよい。さらに、複数の秘密鍵記憶部や複数の暗号器・復号器を1個の半導体ICに形成された回路で実現してもよい。

(4) また、本実施形態では、秘密鍵選択部104はランダムに秘密鍵を選択したが、このような選択方式に限られず、例えば、予め定められた優先順位に従って秘密鍵を選択し、もしその秘密鍵が解読された場合に他の秘密鍵を選択することとしてもよい。

(5) また、本実施形態では、各グループに2個ずつ秘密鍵が配布され、それらから選択された1個だけが暗号化に用いられたが、このような数値に限定されない。例えば、送信装置100は、各グループについて配布された4個の秘密鍵から選択した3個の秘密鍵を結合したもの(例えばビットごとの排他的論理和をとったもの)を暗号鍵として暗号文を生成し、各受信装置は、その暗号文に対して、4個の秘密鍵から選択可能な3個の秘密鍵の組み合わせ全てについてそれら3個の秘密鍵のビットごとの排他的論理和によって得られるものを復号鍵としてそれぞれ復号化することで本実施形態と同じ判定を行い、少なくとも1組の復号鍵について上述の2つの復号文Mn及びMnnが一致した場合に、その一致に係る秘密鍵の組合せが送信装置100で選択されたものと判断すればよい。

(6) さらに、本実施形態では、2台以上の受信装置によって1つのグループが形成されたが、各グループに属する受信装置は1台であってもよい。つまり、受信装置ごとに異なる2個以上の秘密鍵を配布しておき、送信装置は、受信装置ごとに異なる秘密鍵を用いた暗号文を送信してもよい。

(実施の形態2)次に、本発明に係る暗号通信システムの実施の形態2について図面を用いて詳細に説明する。本暗号通信システムは、3階層の暗号化を行うことを特徴とする。

〔暗号通信システムの構成〕図6は、実施形態2に係る暗号通信システム全体のシステム構成と暗号通信の原理を説明するための図である。

【0056】本システムは、3階層の暗号化によってデジタル著作物等の著作権を保護せんとする暗号通信システムであり、DVD (Digital Video/Versatile Disc) 310用の記録装置300と再生装置320とから構成される。記録装置300は、デジタルデータをDVD310に記録する装置であり、マスター鍵(Km)記憶部301と、媒体鍵(Kd)生成部302と、タイトル鍵(Kt)生成部303と、3種類の暗号器305~307と、文書、画像、音声等のデジタルデータを記憶するデジタル著作物304とを備える。

【0057】マスター鍵記憶部301は、マスター鍵Km、即ち、正規の(再生が許可された)再生装置320と共有し合う秘密鍵を予め保持し、媒体鍵生成部302は、媒体鍵Kd、即ち、個々のDVD310を区別するための秘密鍵を生成し、タイトル鍵生成部303は、タイトル鍵Kt、即ち、DVD310に記録するデジタル著作物304のタイトル(例えば1本の映画)ごとに付与する秘密鍵を生成する。

【0058】3個の暗号器305~307は、それぞれ、異なる秘密の暗号アルゴリズムE1、E2、E3に基づいて、媒体鍵Kd、タイトル鍵Kt、デジタル著作物Dataを暗号化し、それぞれ暗号化媒体鍵311、暗号化タイトル鍵312、暗号化デジタル著作物313を生成する。再生装置320は、記録装置300によって記録されたDVD310の暗号化デジタル著作物313を読み出して復号化する正規の装置であり、記録装置300が備えるマスター鍵記憶部301と同一のマスター鍵Kmを記憶するマスター鍵Km記憶部321と、3個の復号器322~324とを備える。

【0059】3個の復号器322~324は、それぞれ、記録装置300が備える暗号器305、306、307の暗号アルゴリズムE1、E2、E3の逆変換である秘密の復号アルゴリズムD1、D2、D3に基づいて、DVD310から読み出された暗号化媒体鍵311、暗号化タイトル鍵312、暗号化デジタル著作物313を復号化する。

〔暗号通信システムの動作〕以上のように構成された本暗号通信システムの動作について図6に従って説明する。

【0060】記録装置300においては、以下の3階層の暗号化が行われる。つまり、暗号器305はマスター鍵記憶部301から読み出したマスター鍵Kmを暗号鍵として媒体鍵生成部302で生成された媒体鍵Kdを暗

号化することで暗号化媒体鍵E1(Kd, Km)311を生成し、暗号器306はその媒体鍵Kdを暗号鍵としてタイトル鍵生成部303で生成されたタイトル鍵Ktを暗号化することで暗号化タイトル鍵E2(Kt, Kd)312を生成し、暗号器307はそのタイトル鍵Ktを暗号鍵としてデジタル著作物Data304を暗号化することで暗号化デジタル著作物E3(Data, Kt)313を生成する。

【0061】生成された暗号化媒体鍵E1(Kd, Km)311、暗号化タイトル鍵E2(Kt, Kd)312、暗号化デジタル著作物E3(Data, Kt)313は、記録装置300によってDVD310の所定箇所に記録される。一方、再生装置320においては、以下の3階層の復号化が行われる。つまり、DVD310に記録された暗号化媒体鍵E1(Kd, Km)311、暗号化タイトル鍵E2(Kt, Kd)312、暗号化デジタル著作物E3(Data, Kt)313が再生装置320によって読み出された後に、まず、復号器322はマスター鍵Km記憶部321から読み出したマスター鍵Kmを復号鍵として暗号化媒体鍵E1(Kd, Km)311を復号化することで媒体鍵Kdを生成する。これは、以下の式6より明らかである。

【0062】

$$Kd = D1(E1(Kd, Km), Km) \quad \text{—式6}$$

続いて、復号器323は、復号器322によって生成された媒体鍵Kdを復号鍵として暗号化タイトル鍵E2(Kt, Kd)312を復号化することでタイトル鍵Ktを生成する。これは、以下の式7より明らかである。

$$Kt = D2(E2(Kt, Kd), Kd) \quad \text{—式7}$$

最後に、復号器324は、復号器323によって生成されたタイトル鍵Ktを復号鍵として暗号化デジタル著作物E3(Data, Kt)313を復号化することでデジタル著作物Dataを生成する。これは、以下の式8より明らかである。

【0063】

$$Data = D3(E3(Data, Kt), Kt) \quad \text{—式8}$$

ここで、もし、再生装置320が備えるマスター鍵Kmが記録装置300が備えるマスター鍵Kmと一致しないものである場合には、復号器322から生成された鍵は、もはや記録装置300が備えるタイトル鍵Ktと一致しなくなる。従って、残る2階層の復号化が行われても、復号器324から出力されるデータは、元のデジタル著作物Data304とは一致しない。

【0064】つまり、記録装置300が備えるマスター鍵Kmと同じマスター鍵を備える再生装置320だけが元のデジタル著作物304を得ることができる。以上のように、本暗号通信システムによれば、DVD310にはデジタル著作物304が暗号化されて記録されており、その暗号化デジタル著作物313を読み出して復号できるのは、マスター鍵Kmを備える再生装置320に

限定される。そして、DVD310には更にDVD310ごとに固有の媒体鍵Kd及びデジタル著作物304のタイトルごとに固有のタイトル鍵Ktが暗号化されて記録されており、これらを順次に復号化することに成功して初めて特定のタイトルに係るデジタル著作物Dataの復号化に成功する。

【0065】つまり、記録媒体に全ての暗号鍵が保存されることによる暗号鍵の漏洩やデッドコピー等の不具合・不正が防止されると共に、コンテンツの再生が許可された再生装置とそうでないものとの区別を設ける等の管理が容易となる。

(実施の形態3) 次に、本発明に係る暗号化装置の実施の形態3について図面を用いて詳細に説明する。本暗号装置は、秘密鍵をそのまま用いるのではなく、修正を加えて得られる修正秘密鍵を用いて暗号化することの特徴とする。

〔暗号化装置の構成〕図7は、実施形態3に係る暗号化装置400の構成を示すブロック図である。

【0066】暗号化装置400は、デジタル著作物402を暗号化して送信する装置であり、タイトル鍵Kt生成部401、デジタル著作物402、修正部403、分離部404、暗号器405及び結合部406を備える。タイトル鍵Kt生成部401、デジタル著作物402及

$$E(Data2, Kp) = E(Data2, Kt(+)\text{Data1}) \quad \text{—式10}$$

結合部406は、ラッチ回路等からなり、分離部404から送られてきた分離データData1と、暗号器405から送られてきた暗号文E(Data2, Kp)とを結合することで、元のブロックデータDataに対応する暗号化ブロックデータEdataを出力する。

【0070】図8は、暗号化される前のブロックデータData及び暗号化された後のブロックデータEdataの構造を示す図である。分離データData1はそのまま変化しないが、分離データData2は、分離データData1によって修正されたタイトル鍵Kpで暗号化される。以上のように、本暗号化装置400によれば、秘密鍵は、そのまま暗号鍵として用いられるのではなく、修正を受けた後に用いられる。そして、その修正内容は、暗号化の対象となるデジタル著作物の一部が用いられる。

【0071】これによって、最終的な暗号鍵はコンテンツに依存して決定されることになり、不正な第三者による秘密鍵の推定を困難にすると共に、秘密鍵だけが漏洩することによって他の全てのコンテンツが解読されてしまうという最悪自体の発生も回避される。

【0072】

〔発明の効果〕以上の説明から明らかなように、本発明に係る暗号通信システムは、1台の送信装置と複数のグループ化された受信装置からなる暗号通信システムであって、各グループには相異なる複数の秘密鍵から重複しないで選択した2個以上の秘密鍵を予め配布しておき、その送信装置は、各グループについて1個ずつ選択した

び暗号器405は、実施形態2におけるタイトル鍵生成部303、デジタル著作物304及び暗号器307と同一である。

【0067】分離部404は、ラッチ回路等からなり、デジタル著作物402から取り出したブロックデータDataのうち、暗号化しない部分(分離データData1)と暗号化する部分(分離データData2)とに分離し、前者を修正部403及び結合部406に送り、後者を暗号器405に送る。修正部403は、排他的論理和回路等からなり、タイトル鍵Kt生成部401で生成されたタイトル鍵Ktと、分離部404から送られてきた分離データData1とのビットごとの排他的論理和を算出し、その結果得られたものを以下の式9に示される修正タイトル鍵Kpとして暗号器405に送る。

$$Kp = Kt(+)\text{Data1} \quad \text{—式9}$$

なお、記号(+)は、排他的論理和を示す演算子である。暗号器405は、修正部403から送られてきた修正タイトル鍵Kpを暗号鍵とし分離部404から送られてきた分離データData2を秘密の暗号アルゴリズムEに基づいて暗号化し、得られた暗号文E(Data2, Kp)を結合部406に送る。この暗号文E(Data2, Kp)は、上記式9より、以下の式10の如く表現される。

【0069】

$$E(Data2, Kp) = E(Data2, Kt(+)\text{Data1}) \quad \text{—式10}$$

秘密鍵それぞれを用いて1つの平文を暗号化し、得られた暗号文を対応するグループに属する受信装置に送信する。受信装置それぞれは、受信した暗号文に対して自己が属するグループに配布された複数の秘密鍵それぞれを用いて復号化し、得られた復号文それぞれについて一定の規則性が存在するか否かを判断することで、正しい復号文を特定する。

【0073】これにより、もし1個の秘密鍵が解読された場合であっても、その秘密鍵が配布されたグループとは異なるグループについての暗号通信は影響を受けることなく継続することができる。また、解読された秘密鍵が配布されたグループについては、残る他の秘密鍵を用いて暗号通信を継続することも可能である。さらに、送信装置は各グループについて用いる秘密鍵を任意に変更することができるので、繰り返し同じ秘密鍵を用いることが回避され、第三者による秘密鍵の解読は困難となる。

【0074】つまり、第三者の攻撃による秘密鍵の推定を困難にすると共に、秘密鍵が解読された場合のシステムへの影響を小さく抑えることが可能な暗号通信システムが実現される。ここで、送信装置は、前記規則性を示す暗号文を前記暗号文に添付して各受信装置に送信してもよい。

【0075】これによって、受信装置が複数の復号文の中から正しいものを特定する際の判断基準は暗号化されて送信装置から受信装置に伝送されるので、送信装置が

選択した1個の秘密鍵がいずれであるかという情報も隠
べいされ、安全性の高い暗号通信が実現される。

【図面の簡単な説明】

【図1】本発明の実施形態1に係る暗号通信システム全
体の構成と暗号通信の原理を説明するための図である。

【図2】同暗号通信システムにおける送信装置10と1
台の受信装置20aについての詳細な接続と構成を示す
ブロック図である。

【図3】送信装置100の動作手順を示すフローチャ
ートである。

【図4】受信装置A1の動作手順を示すフローチャ
ートである。

【図5】本発明に係る暗号通信システムの通信媒体が記
録媒体である場合における、その記録媒体に書き込まれ
る内容を示す図である。

【図6】本発明の実施形態2に係る暗号通信システム全
体の構成と暗号通信の原理を説明するための図である。

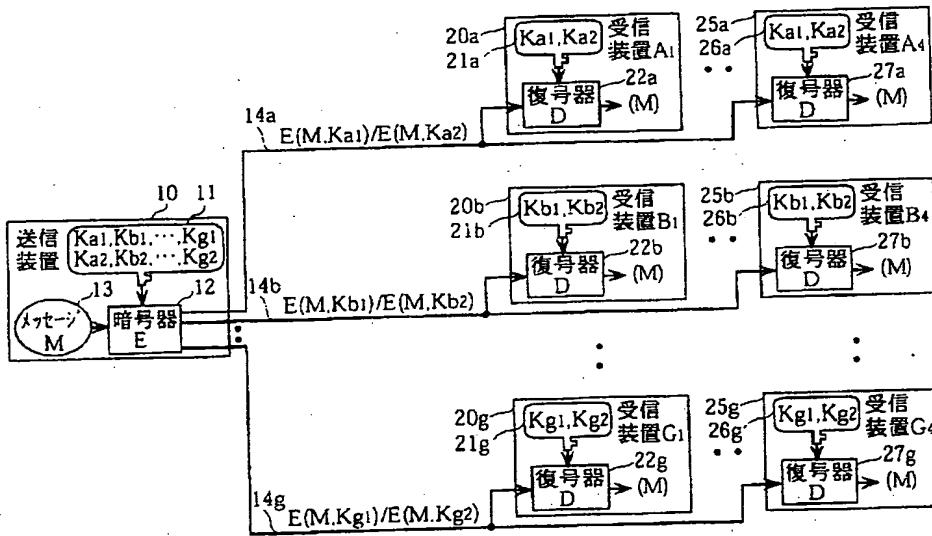
【図7】本発明の実施形態3に係る暗号化装置の構成を
示すブロック図である。

【図8】同暗号化装置によって暗号化される前のプロッ
クデータData及び暗号化された後のブロックデータE
daの構造を示す図である。

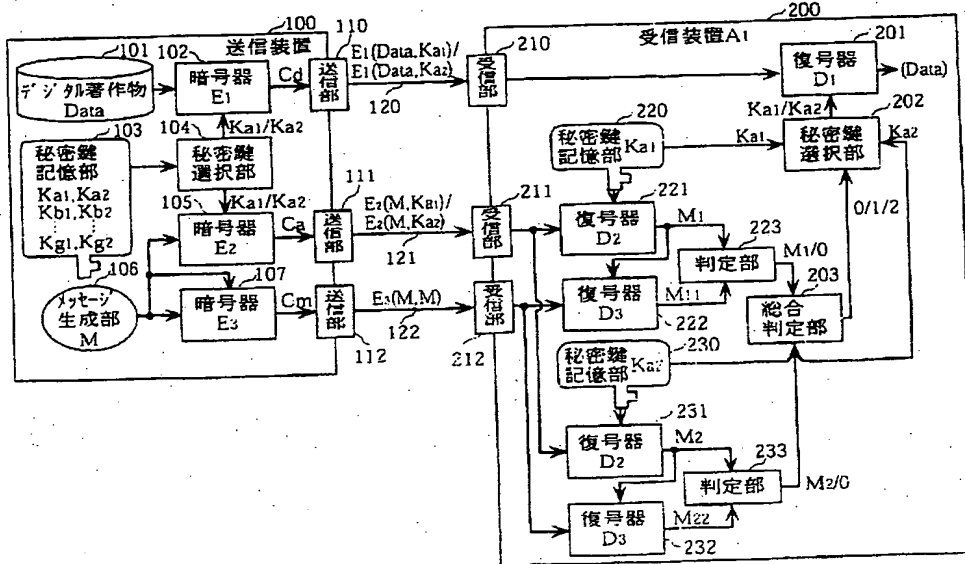
【符号の説明】

- | | | | |
|-----------------|-----------------|---------|-------------|
| 10 | 送信装置 | 105 | 暗号器E2 |
| 11 | 秘密鍵 | 106 | メッセージ生成部 |
| 12 | 暗号器 | 107 | 暗号器E3 |
| 13 | メッセージ | 110~112 | 送信部 |
| 14a~14g | バスライン | 120~122 | バスライン |
| 20a、25a | グループAの受信装置A1、A4 | 201 | 復号器D1 |
| 20b、25b | グループBの受信装置B1、B4 | 202 | 秘密鍵選択部 |
| 20g、25g | グループGの受信装置G1、G4 | 203 | 総合判定部 |
| 21a、26a | グループA用の秘密鍵 | 210~212 | 受信部 |
| 21b、26b | グループB用の秘密鍵 | 220 | 秘密鍵(Ka1)記憶部 |
| 21c、26c | グループC用の秘密鍵 | 221 | 復号器D2 |
| 22a~22g、27a~27g | 復号器 | 222 | 復号器D3 |
| 100 | 送信装置 | 223 | 判定部 |
| 101 | デジタル著作物 | 230 | 秘密鍵(Ka2)記憶部 |
| 102 | 暗号器E1 | 231 | 復号器D2 |
| 103 | 秘密鍵記憶部 | 232 | 復号器D3 |
| 104 | 秘密鍵選択部 | 233 | 判定部 |
| | | 250 | CD-ROM |
| | | 251~257 | 記録領域 |
| | | 300 | 記録装置 |
| | | 301 | マスター鍵記憶部 |
| | | 302 | 媒体鍵生成部 |
| | | 303 | タイトル鍵生成部 |
| | | 304 | デジタル著作物 |
| | | 305~307 | 暗号器E1~E3 |
| | | 310 | DVD |
| | | 311 | 暗号化媒体鍵 |
| | | 312 | 暗号化タイトル鍵 |
| | | 313 | 暗号化デジタル著作物 |
| | | 320 | 再生装置 |
| | | 321 | マスター鍵記憶部 |
| | | 322~324 | 復号器D1~D3 |
| | | 400 | 暗号化装置 |
| | | 401 | タイトル鍵生成部 |
| | | 402 | デジタル著作物 |
| | | 403 | 修正部 |
| | | 404 | 分離部 |
| | | 405 | 暗号器E |
| | | 406 | 結合部 |

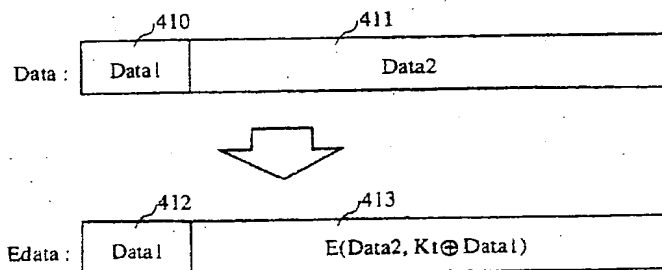
【図1】



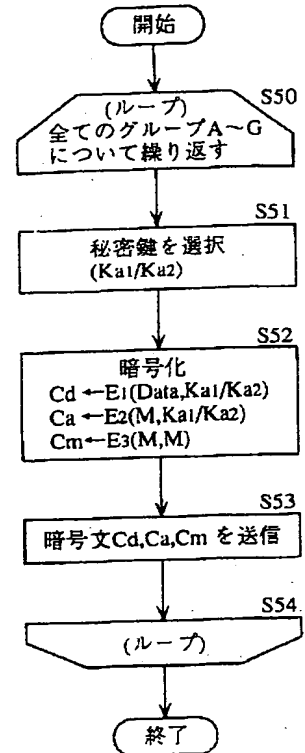
【図2】



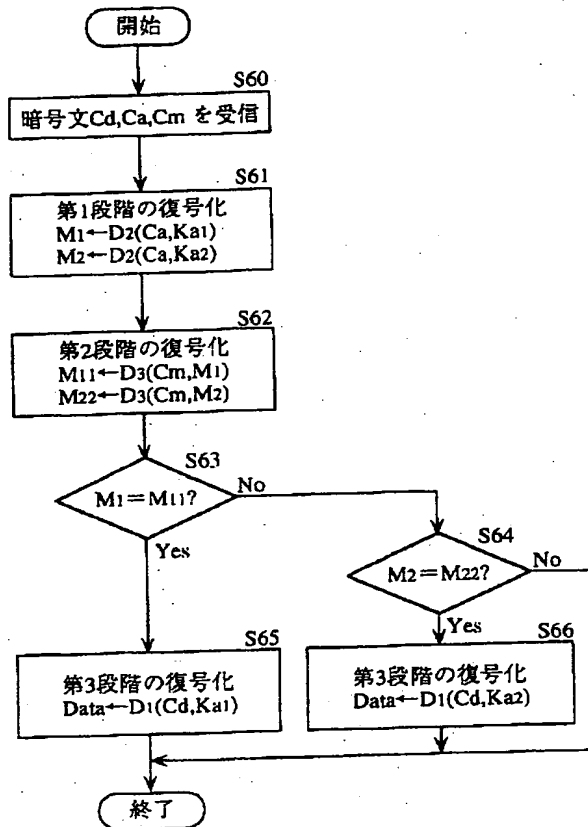
【図8】



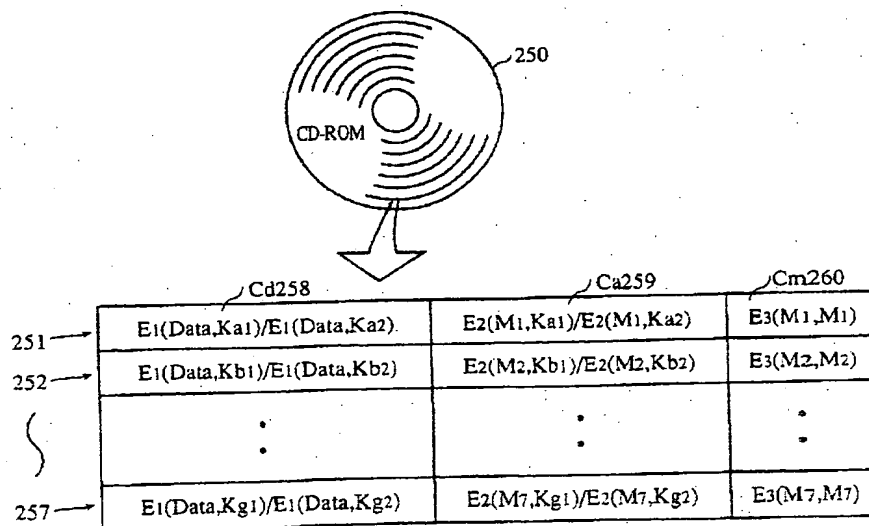
【図3】



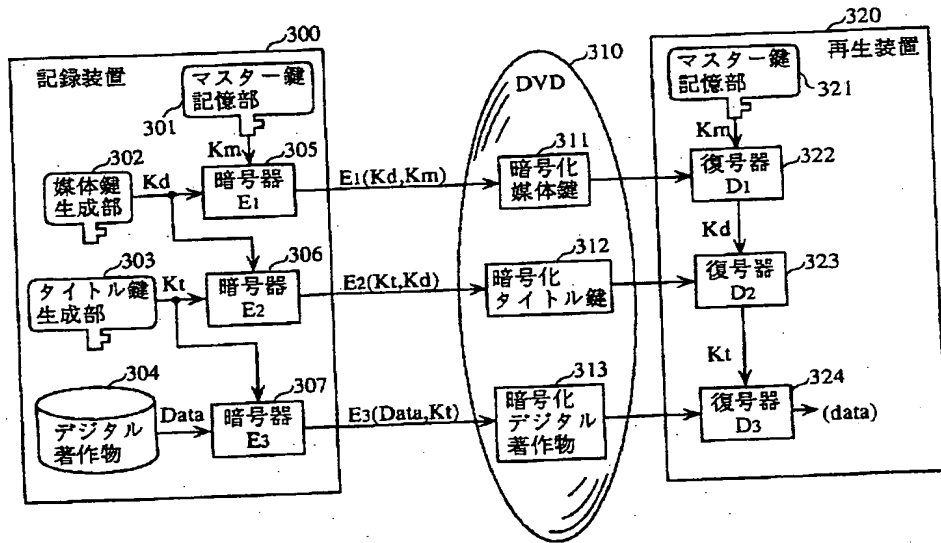
【図4】



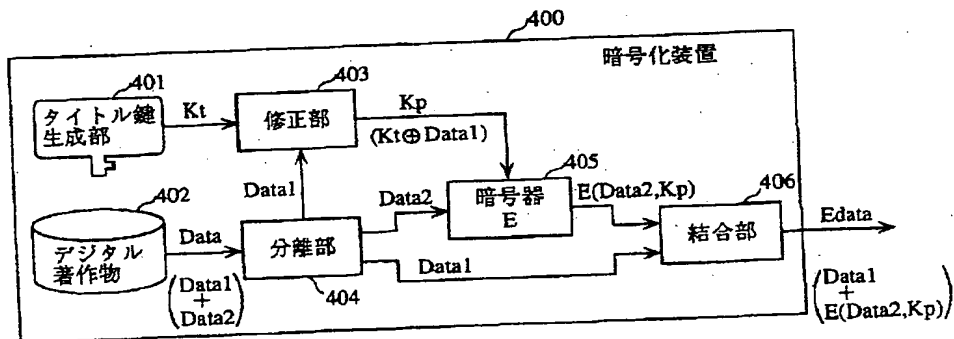
【図5】



【図6】



【図7】



フロントページの続き

(72)発明者 加藤 岳久
神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内

(72)発明者 遠藤 直樹
神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内

(72)発明者 平山 康一
神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.